

Method and System for Granting Access to Information for Electronic Commerce

Abstract of the Disclosure

To reduce the number of key pairs that must be managed in an asymmetric encryption/decryption system, each customer of a vendor is assigned to at least one defined customer group as a function of the information that is to be made available to the customer. A key pair consisting of a group source key and a group member key is assigned to each defined customer group. The vendor uses the group source key to encrypt information to be made available only to members of the associated group. Authenticated customers are given the group member key for each group to which they belong. The customers use the group member key to decrypt information previously encrypted by the vendor using the associated group source key.

CA9-2000-0024US1